GENERAL COMMITTEE MEETING

Thursday, November 15, 2018

3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference Line: 888-432-1688, Room: 6597, User: 6328

1. Welcome and Introductions
2. Coalition Principles **Page 1**
3. 42 CFR Part 2
4. Regulation of data not covered by HIPAA **Pages 2-4 (Wyden Attachment)**
5. Accounting of Disclosures Survey **Pages 5-7**
6. HHS Data Mining Meeting
7. NIST RFI: *Privacy Framework* **Pages 8-18**
8. NTIA Comments: *Developing the Administration's Approach to Consumer Privacy*
   - European Union **Pages 19-24**
   - Federal Trade Commission **Pages 25-45**
9. TCPA Lawsuit **Page 46**

CONFIDENTIALITY COALITION

PRINCIPLES ON PRIVACY

1. Confidentiality of personal health information is of the utmost importance in the delivery of healthcare. All care providers have a responsibility to take necessary steps to maintain the trust of the patient as we strive to improve healthcare quality.

2. Private health information should have the strictest protection and should be supplied only in circumstances necessary for the provision of safe, high-quality care and improved health outcomes.

3. The framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule should be maintained. HIPAA established a uniform framework for acceptable uses and disclosures of individually-identifiable health information within healthcare delivery and payment systems for the privacy and security of health information.

4. The Privacy Rule requires that healthcare providers and health plans use the minimum necessary amount of personal health information to treat patients and pay for care by relying on patients' "implied consent" for treatment, payment of claims, and other essential healthcare operations. This model has served patients well by ensuring quick and appropriate access to medical care, especially in emergency situations where the patient may be unable to give written consent.

5. Personal health information must be secured and protected from misuses and inappropriate disclosures under applicable laws and regulations. Strict enforcement of violations is essential to protect individuals' privacy.

6. Providers should have as complete a patient's record as necessary to provide care. Having access to a complete and timely medical record allows providers to remain confident that they are well-informed in the clinical decision-making process.

7. A privacy framework should be consistent nationally so that providers, health plans, and researchers working across state lines may exchange information efficiently and effectively in order to provide treatment, extend coverage, and advance medical knowledge, whether through a national health information network or another means of health information exchange.

8. The timely and accurate flow of de-identified data is crucial to achieving the quality-improving benefits of a national health information exchange while protecting individuals' privacy. Federal privacy policy should continue the HIPAA regulations for the de-identification and/or aggregation of data to allow access to properly de-identified information. This allows researchers, public health officials, and others to assess quality of care, investigate threats to the public's health, respond quickly in emergency situations, and collect information vital to improving healthcare safety and quality.

9. To the extent not already provided under HIPAA, privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information. A similar expectation of acceptable uses and disclosures for non-HIPAA covered health information is important in order to maintain consumer trust.

The Consumer Data Protection Act of 2018 Discussion Draft - Senator Wyden

The explosive growth in the collection and sale of consumer information enabled by new technology poses unprecedented risks for Americans' privacy. The government has failed to respond to these new threats:

(1) Information about consumers' activities, including their location information and the websites they visit is tracked, sold and monetized without their knowledge by many entities;
(2) Corporations' lax cybersecurity and poor oversight of commercial data-sharing partnerships has resulted in major data breaches and the misuse of Americans' personal data;
(3) Consumers have no effective way to control companies' use and sharing of their data.

The Federal Trade Commission, the nation's main privacy and data security regulator, currently lacks the authority and resources to address and prevent threats to consumers' privacy.

(1) The FTC cannot fine first-time corporate offenders. Fines for subsequent violations of the law are tiny, and not a credible deterrent.
(2) The FTC does not have the power to punish companies unless they lie to consumers about how much they protect their privacy or the companies' harmful behavior costs consumers money.
(3) The FTC does not have the power to set minimum cybersecurity standards for products that process consumer data, nor does any federal regulator.
(4) The FTC does not have enough staff, especially skilled technology experts. Currently about 50 people at the FTC police the entire technology sector and credit agencies.

The **Consumer Data Protection Act** protects Americans' privacy, allows consumers to control the sale and sharing of their data, gives the FTC the authority to be an effective cop on the beat, and will spur a new market for privacy-protecting services. The bill empowers the FTC to:

(1) Establish minimum privacy and cybersecurity standards.
(2) Issue steep fines (up to 4% of annual revenue), on the first offense for companies and 10-20 year criminal penalties for senior executives.
(3) Create a national Do Not Track system that lets consumers stop third-party companies from tracking them on the web by sharing data, selling data, or targeting advertisements based on their personal information. It permits companies to charge consumers who want to use their products and services, but don't want their information monetized.
(4) Give consumers a way to review what personal information a company has about them, learn with whom it has been shared or sold, and to challenge inaccuracies in it.
(5) Hire 175 more staff to police the largely unregulated market for private data.
(6) Require companies to assess the algorithms that process consumer data to examine their impact on accuracy, fairness, bias, discrimination, privacy, and security.

Section-by-Section Analysis and Explanation
Consumer Data Protection Act of 2018

Sec 1. Short Title: "Consumer Data Protection Act"

Section 1 designates the act as the *Consumer Data Protection Act*.

Sec 2. Definitions

Section 2 defines the terms "automated decision system," "automated decision system impact assessment," "covered entity," "personal information," "data protection impact assessment," "high-risk automated decision system," "high-risk information system," "information system," "share," "store," and "use" as they are used in the Consumer Data Protection Act.

Sec 3. Noneconomic Injury

Section 3 expands the FTC's authority by defining "harmful" business practices to include those that create a significant risk of unjustified exposure of personal information.

Sec 4. Civil Penalty Authority

Section 4 authorizes the the FTC to assess civil penalties of up to $50,000 per violation and 4% of the entity's total annual gross revenue against violators of the Consumer Data Protection Act including for first time violations.

Sec 5. Annual Data Protection Reports

Section 5 requires the senior executives (Chief Executive Officer, Chief Privacy Officer, Chief Information Security Officer) of companies with more than a billion dollars per year of revenue or data on more than 50 million consumers to file annual reports with the FTC detailing whether or not the company complied with the privacy and data security regulations created by the Consumer Data Protection Act. This section also creates criminal penalties, including imprisonment of up to 20 years, if these executives sign off on false statements in these annual reports.

Sec 6. "Do Not Track" Data-Sharing Opt-Out

Section 6 authorizes the FTC to establish a national system to provide consumers with a way to opt-out of companies' sharing their personal information. Companies that wish to continue to share consumer's personal data after the consumer opted-out will be able to ask consumers for permission to do so, and if those companies want require that as a condition of offering their product or service, they will also need to offer a paid version of

their product or service, for which they can charge no more than they would have made by sharing the user's data.

Sec 7. Data Protection Authority

Section 7 authorizes the Federal Trade Commission (FTC) to create regulations that (1) establish and implement minimum privacy and cybersecurity standards, (2) give consumers a way to review what personal information a covered entity stores about them, learn with whom it has been shared, and challenge inaccuracies in that information, and (3) require companies conduct impact assessments of their high-risk automated decision systems and high-risk information systems.

Sec 8. Bureau of Technology

Section 8 establishes a Bureau of Technology within the FTC to be staffed by 50 new technical experts.

Sec 9. Additional Personnel in the Bureau of Consumer Protection

Section 9 authorizes the FTC to appoint 100 additional personnel in the Division of Privacy and Identity Protection of the Bureau of Consumer Protection, and 25 additional personnel in the Bureau's Enforcement Division.

Sec 10. Complaint Resolution

Section 10 authorizes the FTC to establish procedures for the resolution of complaints by consumers regarding violations of the Consumer Data Protection Act, which will require the FTC to forward the complaints to the offending companies, and then forward the company's response back to the consumer.

Sec 11. Application Programming Interfaces

Section 11 requires the FTC, in consultation with the National Institute of Standards and Technology, to establish Application Programming Interfaces (APIs) to permit consumers to use apps and other computer programs to request, receive, and process information they are entitled to under this Act, and to manage their opt-out preferences.

Sec 12. News Media Protections

Section 12 clarifies that the obligations imposed on entities under this Act (such as disclosing what information they have about a consumer) do not apply to journalists.

Accounting of Disclosures Calculation of the Impact of New Privacy Rule Requirements

Current Law

Under current HIPAA privacy rules (45 CFR §164.528), individuals have a right to receive within 60 days of the request (with one 30 day extension available) an accounting of disclosures of their protected health information (PHI) made by a covered entity (CE), including disclosures to or by the CE's business associates (BA) for up to six years prior to the date on which the accounting is requested, except for disclosures:

1 for treatment, payment, or health care operations
2 to the individual or his personal representative
3 incident to otherwise permitted or required uses or disclosures
4 pursuant to an authorization
5 for the facility's directory or to persons (e.g. family members) included in the person's care and for disaster relief
6 for national security or intelligence purposes
7 to correctional institutions or law enforcement officials for certain purposes
8 of a limited data set
9 that occurred prior to the compliance date for the CE

For each disclosure, the following must be provided:

1 the date of the disclosure
2 the name of the entity or person who received the PHI and, if known, the address
3 a brief description of the PHI disclosed
4 a brief statement of the purpose of the disclosure or a copy of the request for the disclosure

Multiple disclosures to the same entity or person may be aggregated. For disclosures for research of the PHI of more than 50 individuals the CE may provide summary information about the disclosures (which may or may not include the requesting individual's PHI) and contact information for the researcher and the research sponsor. CEs must provide the first accounting of disclosures report without charge. Reasonable cost-based fees may be imposed for additional requests by the same individual within the 12-month period provided the CE informs the individual in advance of the fee and provides an opportunity for the individual to withdraw or modify the request.

Responding to Requests for an Accounting of Disclosures Report Under Current Law (this information will help assess the current compliance burden and the current level of individuals' interest in accounting of disclosures reports):

1. Approximately how many patients do you annually provide care for, pay claims for, or otherwise serve? _____
2. (a) How many individuals have requested an accounting of disclosures report since 2010?_____
   (b) How many individuals requested an accounting of disclosures report in 2017? _____
3. How many disclosures (please provide an average and/or a range) were listed in the reports you produced? _____
4. How many of the disclosures listed in the reports you produced were for research purposes (average and/or range please)?
_____
5. Generally describe the steps taken to generate an accounting of disclosures report: _____
_____
6. Does your staff proactively document the information specifically required for the report at the time a disclosure is made or do you only retroactively recreate/extract this information from existing documentation at the time a patient requests a report?
_____
7. How many information systems with PHI do you have? _____
8. How many information systems are searched to produce a report? _____
9. (a) How many automated system interfaces do you have that convey PHI between systems (please describe)? _____
   (b) How many of these interfaces convey PHI between separate covered entities? _____
   (c) How many interfaces do you have with Business Associates (please describe)?_____
10. (a) How many authorized users do your information systems with PHI have? _____ (b) Of these authorized users, how many are employed by you or considered part of your workforce? _____ (c) Of these authorized users, how many are affiliated, credentialed providers (e.g., non-employed physicians with privileges at your facility)? _____
11. How many of your information systems currently store audit trail data?_____
12. What elements do your audit trails capture (user id, log on/off, date/time stamp, patient id, description of information accessed, etc)?
_____ _____
13. How long do your audit trails hold information? _____
14. Do your audit trails distinguish between a use and disclosure? If so, how? ?_____
15. (a) Describe how audit trails were utilized to produce the report, if at all? _____ (b) What, if anything, in addition to audit trails, was used to produce the report?_____
_____
16. Approximately how many professional staff hours are needed to compile the report (please provide an average and/or a range)?_____
17. What is the average cost and/or the range of costs incurred to produce a report? _____ _____
_____
18. If known, what prompted individuals to request an accounting of disclosures report? _____
19. Were the requestors satisfied with the accounting of disclosures report? _____

Impact of Expanded Accounting of Disclosures Requirements to Include Disclosures Relating to Treatment, Payment, and Health Care Operations

The HITECH Act, part of the American Recovery and Reinvestment Act of 2009 (the stimulus package), was signed into law by President Obama on February 17, 2009. **Section 13405(c) of the Act newly requires CEs that use or maintain an Electronic Health Record (EHR)[i] to provide, upon request, an accounting of disclosures[ii] made for treatment, payment and health care operations[iii] purposes through an EHR over a three-year period.** In response to a request, CEs may either provide an accounting for disclosures of PHI made by the CE and its business associates or may provide an accounting of disclosures made by the CE and a list of all BAs acting on behalf of the CE including contact information for the BAs. BAs on a CE's list must, in response to a request, provide an accounting of its disclosures.

To calculate the impact of this requirement on Covered Entities and their Business Associates:

1. Is your organization a Covered Entity? If yes, what type of Covered Entity (plan, provider, OHCA, etc) and how many business associates do you have? _____
2. Is your organization a business associate? If yes, please describe your organization: _____
3. Approximately how many disclosures for treatment purposes are made annually?_____
4. Approximately how many disclosures for payment purposes are made annually? _____
5. Approximately how many disclosures for health care operations purposes are made annually?_____
6. The Privacy Rule currently requires that an accounting of disclosures report include the date of the disclosure, a description of the information disclosed, the name (and if known the address) of the entity or person who received the information disclosed, and a statement of the purpose for the disclosure or a copy of the written request for the disclosed information. Anticipating that expanded reporting for treatment, payment and healthcare operations purposes would be similar to current reporting, do you currently have the capacity to produce an accounting of disclosures report that includes such information? _____
7. Would additional storage capacity be required to maintain three years of data on disclosures for treatment, payment and health care operations? _____
   a. If yes, how much additional storage capacity would be required? _____
   b. If yes, what would be the cost of adding this additional storage capacity? _____
8. Would additional programming capacity or infrastructure be required to capture and maintain three years of data on disclosures for treatment, payment and health care operations?_____
   a. If yes, how much additional programming capability would be required?_____
   b. If yes, what would be the cost be of adding this additional capacity? _____
9. Would additional personnel be needed to maintain the capacity to produce accounting of disclosures reports that included disclosures for treatment, payment and health care operations over a three-year period?_____
   a. If yes, how much additional personnel would be needed? _____
   b. If yes, what would be the cost of adding this additional capacity?_____
10. What would you suggest to ease the compliance burden? (e.g., reduce the information required to be collected about each disclosure/eliminate the requirement to account for disclosures made to health care providers who are authorized users of the CEs EHR/allow CEs to charge for the labor cost of creating a report)

_____

_____

11. a. What is the approximate total cost of altering your operations to be able to comply with the expanded accounting of disclosures requirements?_____
    b. How long do you estimate it will take to make these changes to your systems? _____
    c. What is the estimated annual cost of system maintenance? (just the incremental cost for compliance with the new requirements)

_____

    d. How many man hours do you estimate it would take to compile an accounting of disclosures report only for disclosures for treatment, payment and health care operations disclosures? _____

Your Name & Title: _____

Company: _____

Address:_____

Phone Number & Email Address:_____

[1] ***Electronic Health Record*** means an "electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." **(**HITECH Act §13400(5)) [1] ***Disclosure*** means "the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information." This is different from "***use***," which means, "with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information." (45 CFR 160.103) [1] ***Treatment*** means the provision, coordination, or management of healthcare and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. (45 CFR 164.501) ***Payment*** means*:* (1)The activities undertaken by: (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and (2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to: (i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing; (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (A) Name and address; (B) Date of birth; (c) Social security number; (D) Payment history; (E) Account number; and (F) Name and address of the healthcare provider and/or health plan. (45 CFR 164.501) ***Health care operations*** means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable; (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. (iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and (v) Consistent with the applicable requirements of §164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity. (45 CFR 164.501)

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number 181101997-8997-01]

Developing a Privacy Framework

AGENCY: National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION: Notice; Request for Information (RFI)

SUMMARY: The National Institute of Standards and Technology (NIST) is developing a framework that can be used to improve organizations' management of privacy risk for individuals arising from the collection, storage, use, and sharing of their information.[1] The NIST Privacy Framework: An Enterprise Risk Management Tool ("Privacy Framework"), is intended for voluntary use and is envisioned to consist of outcomes and approaches that align policy, business, technological, and legal approaches to improve organizations' management of processes for incorporating privacy protections into products and services. This notice requests information to help identify, understand, refine, and guide development of the Privacy Framework. The Privacy Framework will

[1] While NIST requests information about how organizations define privacy risk in topic #3 below, for the purposes of this RFI, NIST references the privacy risk model set forth in NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at https://csrc.nist.gov/publications/detail/nistir/8062/final, which analyzes the problems that individuals might experience as a result of the processing of their information, and the impact if they were to occur.

be developed through a consensus-driven, open, and collaborative process that will include workshops and other opportunities to provide input.

DATES: Comments in response to this notice must be received by 5:00 PM Eastern time on [PLEASE INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Written comments may be submitted by mail to Katie MacFarland, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899. Electronic submissions may be sent to privacyframework@nist.gov, and may be in any of the following formats: HTML, ASCII, Word, RTF, or PDF. Please cite "Developing a Privacy Framework" in all correspondence. Comments received by the deadline will be posted at http://www.nist.gov/privacyframework without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be posted or considered.

FOR FURTHER INFORMATION CONTACT: For questions about this RFI contact: Naomi Lefkovitz, U.S. Department of Commerce, NIST, MS 2000, 100 Bureau Drive, Gaithersburg, MD 20899, telephone (301) 975-2924, e-mail privacyframework@nist.gov. Please direct media inquiries to NIST's Public Affairs Office at (301) 975-NIST.

SUPPLEMENTARY INFORMATION:

Genesis for the Privacy Framework's Development

It is a challenge to design, operate, or use technologies in ways that are mindful of diverse privacy needs in an increasingly connected and complex environment. Current and cutting-edge technologies such as mobile devices, social media, the Internet of Things and artificial intelligence are giving rise to increased concerns about their impacts on individuals' privacy. Inside and outside the U.S., there are multiple visions for how to

address these concerns. Accordingly, the U.S. Department of Commerce (DOC) is developing a forward-thinking approach that supports both business innovation and strong privacy protections. As part of this effort, NIST is developing a voluntary Privacy Framework to help organizations: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services.[2] The Privacy Framework is intended to be a tool that would assist with enterprise risk management.

Privacy Framework Development and Attributes

While good cybersecurity practices help manage privacy risk through the protection of personally identifiable information (PII),[3] privacy risks also can arise from how organizations collect, store, use, and share PII to meet their mission or business objective, as well as how individuals interact with products and services. NIST seeks to understand whether organizations that design, operate, or use these products and services would be better able to address the full scope of privacy risk with more tools to support better implementation of privacy protections.

NIST will develop the Privacy Framework in a manner consistent with its mission to promote U.S. innovation and industrial competitiveness, and is seeking input from all interested stakeholders. NIST intends for the Framework to provide a prioritized, flexible, risk-based, outcome-based, and cost-effective approach that can be compatible with existing legal and regulatory regimes in order to be the most useful to organizations and

[2] In parallel with this effort, the DOC's National Telecommunications and Information Administration is developing a set of privacy principles in support of a domestic policy approach that advances consumer privacy protections while protecting prosperity and innovation, in coordination with DOC's International Trade Administration to ensure consistency with international policy objectives: https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.

[3] For the purposes of this RFI, NIST is using the definition from the Office of Management and Budget Circular A-130. PII is defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

enable widespread adoption. NIST expects that the Privacy Framework development process will involve several iterations to allow for continuing engagement with interested stakeholders. This will include interactive workshops, along with other forms of outreach.

On October 16, 2018, NIST held its first workshop in Austin, Texas to launch the framework development process.[4] NIST heard from panelists from industry, civil society and academia, as well as audience participants about the needs the Privacy Framework should address and some key desired characteristics. As a consequence, NIST believes that in order to be effective, the Privacy Framework should have the following minimum attributes:

1. **Consensus-driven and developed and updated through an open, transparent process.** All stakeholders should have the opportunity to contribute to the Privacy Framework's development. NIST has a long track record of successfully and collaboratively working with stakeholders to develop guidelines and standards. NIST will model the approach for the Privacy Framework on the successful, open, transparent, and collaborative approach used to develop the Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework").[5]
2. **Common and accessible language.** The Privacy Framework should be understandable by a broad audience, including senior executives and those who are not privacy professionals. The Privacy Framework can then facilitate communications among various stakeholders by promoting use of this common language.
3. **Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses.** The Privacy Framework should be scalable to organizations of all sizes, public or private, in any sector, and operating within or across domestic borders. It should be platform- and technology- agnostic and customizable.

[4] https://www.nist.gov/news-events/events/2018/10/kicking-nist-privacy-framework-workshop-1.

[5] https://www.nist.gov/cyberframework/framework.

4. **Risk-based, outcome-based, voluntary, and non-prescriptive.** The Privacy Framework should provide a catalog of privacy outcomes and approaches to be used voluntarily, rather than a set of one-size-fits-all requirements, in order to: foster innovation in products and services; inform education and workforce development; and promote research on and adoption of effective privacy solutions. The Privacy Framework should assist organizations to better manage privacy risks within their diverse environments without prescribing the methods for managing privacy risk.
5. **Readily usable as part of any enterprise's broader risk management strategy and processes.** The Privacy Framework should be consistent with, or reinforce, other risk management efforts within the enterprise, recognizing that privacy is one of several major areas of risk that an organization needs to manage.
6. **Compatible with or may be paired with other privacy approaches.** The Privacy Framework should take advantage of existing privacy standards, methodologies, and guidance. It should be compatible with and support organizations' ability to operate under applicable domestic and international legal or regulatory regimes.
7. **A living document.** The Privacy Framework should be updated as technology and approaches to privacy protection change and as stakeholders learn from implementation.

Although the goal of the Privacy Framework is to help organizations better identify, assess, manage, and communicate privacy risks, NIST expects there may be aspects of privacy practices that are not sufficiently developed for inclusion in the Privacy Framework. When developing the Cybersecurity Framework, NIST produced a related roadmap that identified focus areas that still needed more research and understanding before they were mature enough for widespread adoption, but that could potentially inform future revisions of the Cybersecurity Framework. With respect to the Privacy Framework, NIST anticipates that a roadmap may be needed for similar reasons.

As noted below, NIST solicits comments on the desired attributes of a Privacy Framework, as well as high-priority gaps in organizations' ability to manage privacy risk, as part of this RFI.

Goals of this Request for Information

Based upon discussions that took place during the October 16, 2018 workshop, this RFI seeks further information about the topics discussed by stakeholders, as elaborated in the sections below. The RFI invites stakeholders to submit ideas, based on their experience as well as their mission and business needs, to assist in prioritizing elements and development of the Privacy Framework. NIST invites industry, civil society groups, academic institutions, Federal agencies, state, local, territorial, tribal, and foreign governments, standard-setting organizations, and other interested stakeholders to respond.

The goals of the Privacy Framework development process, generally, and this RFI, specifically, are:

(i) to better understand common privacy challenges in the design, operation, and use of products and services that might be addressed through a voluntary Privacy Framework,

(ii) to gain a greater awareness about the extent to which organizations are identifying and communicating privacy risk or have incorporated privacy risk management standards, guidelines, and best practices, into their policies and practices; and

(iii) to specify high-priority gaps for which privacy guidelines, best practices, and new or revised standards are needed and that could be addressed by the Privacy Framework or a related roadmap.

Details About Responses to This Request for Information

When addressing the topics below, commenters may address the practices of their organization or a group of organizations with which they are familiar. If desired, commenters may provide information about the type, size, and location of the organization(s). Provision of such information is optional and will not affect NIST's full consideration of the comment.

Comments containing references, studies, research, and other empirical data that are not widely published (e.g., available on the Internet) should include copies of or electronic links to the referenced materials. Beyond that, responses should not include additional information. Do not include in comments or otherwise submit information deemed to be proprietary, private, or in any way confidential, as all comments relevant to this RFI topic area that are received by the deadline will be made available publicly at http://www.nist.gov/privacyframework.

Request for Information

The following list of topics covers the major areas about which NIST seeks information. The listed areas are not intended to limit the topics that may be addressed by respondents so long as they address privacy and how a useful Privacy Framework might be developed. Responses may include any topic believed to have implications for the development of the Privacy Framework, regardless of whether the topic is included in this document.

Risk Management

NIST solicits information about how organizations assess risk; how privacy considerations factor into that risk assessment; the current usage of existing privacy standards, frameworks, models, methodologies, tools, guidelines, and principles; and other risk management practices related to privacy. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in achieving NIST's goal of developing a framework that includes and identifies common practices across contexts and environments and is structured to help organizations achieve positive privacy outcomes. Accordingly, NIST is requesting information related to the following topics:

Organizational Considerations

1. The greatest challenges in improving organizations' privacy protections for individuals;

2. The greatest challenges in developing a cross-sector standards-based framework for privacy;
3. How organizations define and assess risk generally, and privacy risk specifically;
4. The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management;
5. Current policies and procedures for managing privacy risk;
6. How senior management communicates and oversees policies and procedures for managing privacy risk;
7. Formal processes within organizations to address privacy risks that suddenly increase in severity;
8. The minimum set of attributes desired for the Privacy Framework, as described in the *Privacy Framework Development and Attributes* section of this RFI, and whether any attributes should be added, removed or clarified;
9. What an outcome-based approach to privacy would look like;
10. What standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles organizations are aware of or using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels, and whether any of them currently meet the minimum attributes described above;
11. How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles;
12. Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices;
13. The role(s) national/international standards and organizations that develop national/international standards play or should play in providing confidence mechanisms for privacy standards, frameworks, models, methodologies, tools, guidelines, and principles;
14. The international implications of a Privacy Framework on global business or in policymaking in other countries; and

15. How the Privacy Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform privacy functions within organizations.

Structuring the Privacy Framework

NIST is interested in understanding how to structure the Privacy Framework to achieve the desired set of attributes and improve integration of privacy risk management processes with the organizational processes for developing products and services for better privacy outcomes. NIST is seeking any input from the public regarding options for structuring the Privacy Framework, and is particularly interested in receiving comment on the following issues, if applicable:

16. Please describe how your organization currently manages privacy risk. For example, do you structure your program around the information life cycle (i.e., the different stages – from collection to disposal – through which PII is processed), around principles such as the fair information practice principles (FIPPs), or by some other construct?
17. Whether any aspects of the Cybersecurity Framework could be a model for this Privacy Framework, and what is the relationship between the two frameworks.
18. Please describe your preferred organizational construct for the Privacy Framework. For example, would you like to see a Privacy Framework that is structured around:
    a. The information life cycle;
    b. Principles such as FIPPs;
    c. The NIST privacy engineering objectives of predictability, manageability, and disassociability[6] or other objectives;
    d. Use cases or design patterns;
    e. A construct similar to the Cybersecurity Framework functions, categories, and subcategories; or
    f. Other organizing constructs?

[6] NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at https://csrc.nist.gov/publications/detail/nistir/8062/final.

Please elaborate on the benefits or challenges of your preferred approach with respect to integration with organizational processes for managing enterprise risk and developing products or services. If you provided information about topic 10 above, please identify any supporting examples of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles.

Specific Privacy Practices

In addition to the approaches above, NIST is interested in identifying core privacy practices that are broadly applicable across sectors and organizations. NIST is interested in information on the degree of adoption of the following practices regarding products and services:

- De-identification;
- Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared;
- Enabling user preferences;
- Setting default privacy configurations;
- Use of cryptographic technology to achieve privacy outcomes – for example, the disassociability privacy engineering objective;
- Data management, including:
  - Tracking permissions or other types of data tracking tools,
  - Metadata,
  - Machine readability,
  - Data correction and deletion; and
- Usable design or requirements.

19. Whether the practices listed above are widely used by organizations;
20. Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework;
21. How the practices listed above or other proposed practices relate to existing international standards and best practices;

22. Which of these practices you see as being the most critical for protecting individuals' privacy;
23. Whether some of these practices are inapplicable for particular sectors or environments;
24. Which of these practices pose the most significant implementation challenge, and whether the challenges vary by technology or other factors such as size or workforce capability of the organization;
25. Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence; and
26. How standards or guidelines are utilized by organizations in implementing these practices.

Authority: 15 U.S.C. 272(b), (c), & (e); 15 U.S.C. 278g-3.

Kevin A. Kimball,
Chief of Staff.

[FR Doc. 2018-24714 Filed: 11/13/2018 8:45 am; Publication Date: 11/14/2018]

Ref. Ares(2018)5744896 - 09/11/2018

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C: Fundamental rights and rule of law
Unit C.4: International data flows and protection

Brussels, 9 November 2018
JUST.C.4/CM

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725, Attn: Privacy RFC
Washington, DC 20230

Submitted by e-mail to: privacyrfc2018@ntia.doc.gov

Subject: Request for public comments on a proposed approach to consumer privacy [Docket No. 180821780-8780-01]

Dear Assistant Secretary Redl,

We have read with great interest the recent publication and request for public comments by the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce on proposed privacy outcomes and high-level goals for Federal action on consumer privacy.

The EU and the United States have a very close relationship and long-standing cooperation in a number of areas that increasingly rely on transatlantic data flows, including trade, regulatory and law enforcement cooperation. A common set of data protection principles has already been agreed between the EU and the United States in both the commercial field (the "EU-US Privacy Shield" framework[1]) and the law enforcement area (the "Data Protection and Privacy Agreement" or "DPPA"[2]). In building on these principles and increasing convergence between our approaches towards data protection, we can help to facilitate data exchanges while further strengthening these instruments.

Against that background and given that, in the past years, the EU has gone through a similar process of consulting stakeholders and reforming our privacy rules, we appreciate

[1] See Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

[2] Agreement between the EU and the U.S. on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters (in the EU referred to as "Umbrella Agreement").

the opportunity to submit the comments below. We understand that this consultation covers only the first step in a process that might lead to Federal action and would therefore like to express our readiness to provide further comments on a more developed proposal in the future.

In our view, and as increasingly accepted globally, the basic architecture of a modern, balanced and flexible privacy regime is characterised by four key elements: an overarching law; a core set of data protection principles; enforceable individual rights; and finally, an independent supervisory authority with effective powers to ensure the enforcement of those rules. We welcome that these elements are also at the core of NTIA's proposed approach to consumer privacy, and have therefore structured our comments broadly around those four aspects:

- First, we note that one of the high-level goals identified by NTIA is the **harmonisation of the regulatory landscape** through a set of overarching principles that would apply to all business activities previously not covered by sectoral laws. Given the considerable increase in the use and exchange of data, including personal information, across all sectors of the economy – with the consequence that sectoral laws thus cannot provide the necessary legal certainty to business organizations nor ensure the necessary protection of consumers – this would be significant progress. Overcoming the current regulatory fragmentation would create a level playing field, ensuring that data can move easily between operators, industries and business models on the basis of clear and harmonised rules while guaranteeing a consistent protection of individuals. In line with the existing sectoral rules and as a reflection of the fundamental value of privacy, we believe that these comprehensive principles and safeguards should be enshrined in a legislative instrument and not be left to soft law instruments or self-regulation. Doing so does not affect the necessary flexibility as statutory rules still leave space for further clarification through interpretative guidance, taking into account lessons learnt and technological developments.

- Second, we fully share the view of NTIA that **trust** should be at the core of the U.S. (and in fact any) privacy policy formulation. We strongly believe that, giving individuals more control over their own data will increase trust in the way businesses handle their data, with the result that individuals will be more willing to share their information and use services. This trust, particularly in the online environment, is essential to support the development of the digital economy. Conversely, if individuals are afraid that others will not respect their privacy or fail to guarantee the security of their data, they will lose confidence and become averse to certain forms of online activities. Ensuring trust should therefore guide the development of all data protection principles and safeguards.

- Third, we very much welcome that the seven user-centric privacy outcomes proposed by NTIA cover **core data protection principles** that have been developed since the 1970's and are now widely shared across the world. For instance, the principles of "reasonable minimization", "security", "transparency" and "accountability" are essential safeguards but also reflect sound data management (and thus good business practice). At the same time, we note that certain other core principles are currently not explicitly reflected in NTIA's proposed privacy outcomes. These include for instance the principle of **lawful data processing** (i.e. the need for a legal basis), the requirement to process personal data only for **specific purposes** (and further process it for purposes that are not incompatible with the original purposes), a central reference point also for other principles (e.g. that of limited data retention); the requirement that

personal data should be **accurate** and **relevant** for the purposes for which they are processed; and specific protections for **"sensitive data"** (i.e. personal data for which there is a particularly high risk that they could become grounds for discrimination, e.g. religious beliefs, sexual orientation or health conditions). These principles are not only widely accepted as key elements of modern data protection legislation, including to ensure individuals' greater confidence in the way their data are collected and handled, but have also been codified in important recent instruments agreed between the EU and the United States.[3]

- Fourth, in our view, **effective safeguards and enforceable individual rights** are key components of a modern data protection regime.

  We therefore very much welcome that, according to the RFC, the desired outcome of consumer privacy in the United States would revolve around the information and empowerment of the consumer, in particular by ensuring **transparency** and **control** of his/her data. Individuals should be clearly informed about what happens to their data (what data is processed, for which purposes, who is processing the data, with whom might it be shared, etc.), including in case their data is stolen or lost (data breach). In this respect, since these incidents can have very harmful consequences (identity theft, fraud, etc.) it might be useful to include a requirement to **report data breaches**. This is a key safeguard enabling individuals to protect themselves from (or at least mitigate) potential harm already recognised for instance in the DPPA (Article 10). While we understand that data breaches laws have been enacted by States, businesses and individuals could benefit from the harmonisation of the conditions for the notification of such incidents.

  Putting individuals in control of their personal data also presupposes that they benefit from a clear set of enforceable rights to effectively exercise such control. In this regard, we welcome the inclusion in the RFC of core data protection rights such as the right to access and correction. In addition, with a view to addressing particular challenges of the digital world, it might be worth considering going beyond those 'classic' rights. For instance, there is a need to specifically protect individuals when they are significantly impacted by decisions based solely on automated processing (e.g. the rejection of an online credit, or an e-recruiting application). **Automated individual decision-making** and profiling have great potential to speed up decisions, make them more informed and objective. At the same time, they can also pose risks for individuals, for instance if the underlying algorithms are 'biased'. Given the increasing relevance of the use of algorithms in data processing, the 'traditional' rights of access, correction and erasure might be insufficient to ensure effective control of individuals over their data and protect them against discrimination. Therefore, while we understand that certain protections already exist in sectoral laws, we would recommend considering a requirement to explain the underlying logic of automated decisions and a right for individuals to ask for such decisions to be reviewed by a human being when such decisions can have legal effects or otherwise significantly affect them. Again, this is a right already recognised for instance in the DPPA (Article 15).

---

[3] See for example the Choice, Data Integrity and Purpose Limitation Principles (Privacy Principles 2, 5) of the EU-US Privacy Shield and Articles 6, 8, 12, 13 and 15 of the DPPA.

Last but not least, a key data protection safeguard is to empower individuals to pursue **legal remedies** to effectively enforce their rights, in a timely manner and without prohibitive cost. This includes the right to lodge a complaint and have it resolved[4] as well as the right to effective judicial redress. Given the fundamental importance of data protection as a reflection of human dignity and an element of individuals' autonomy and self-determination, obtaining redress should not be subject to restrictive requirements or burdensome conditions, for instance in terms of harm.

- Fifth, the effective implementation of privacy rules crucially depends on **robust oversight and enforcement by an independent authority**.

In this respect, we welcome the emphasis by NTIA on enforcement by the FTC, including the importance of having the necessary resources, clear statutory authority and direction to enforce consumer privacy. We also note that the FTC has initiated a process of reflection on its current authorities in the area of privacy, which notably looks into the efficacy of the FTC's use of its current remedial authority and the need for any additional tools or powers to adequately deter unfair and deceptive conduct related to privacy and data security. One of the lessons learned from recent scandals about the mishandling of personal data is that we need to get serious about oversight and enforcement, especially as some violations of privacy laws can have particularly negative consequences for individuals and, where they affect the democratic process, society as a whole. Strengthening the **FTC's enforcement role** would also reinforce the foundations of the Privacy Shield, a key instrument that facilitates transatlantic data flows.

Moreover, in our view, it would be important to consider the introduction of affordable mechanisms (provided, for example, in the EU through the role of data protection authorities) ensuring the **effective resolution of individual complaints** that might not necessarily correspond to the FTC's enforcement priorities at any given moment (e.g. because of their limited importance from a strategic point of view, even if the alleged violation might be very relevant for the individual complainant). The existence of such mechanisms could significantly contribute to consumer trust, while ensuring quick resolution of disputes and thus preventing lengthy and costly litigation.

Finally, while we fully agree with the importance of a strong culture of "accountability", we equally believe that, to be credible, a system based on the own responsibility of business operators should be coupled with robust enforcement in case of non-compliance. This includes, as in other areas of law, putting in place credible and sufficiently **deterrent sanctions**.

---

[4] See for instance the EU-US Privacy Shield, which requires certified U.S. companies to respond to individuals within a fixed period of time and to "*address whether the complaint has merit and, if so, how the organization will rectify the problem*" (Supplementary Principles 11.c. and 11.d.i.). If the individual is not satisfied with the reply, (s)he can seek redress with one of the available "*independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at not cost to the individual*" (Privacy Principle 7.i.).

Looking at the overall approach, we share the NTIA's view that data protection rules must not stifle innovation and that strong protections, legal clarity and flexibility are all important elements of a modern privacy regime.

In our experience, **privacy and innovation** are two complementary objectives, rather than mutually exclusive. Data protection rules, if designed properly, can in fact encourage innovation, for example by guaranteeing that data protection safeguards are built into products and services from the earliest stage of development (data protection by design and by default). This incentivises businesses to innovate and develop new ideas, methods and technologies for security and the protection of personal data. We therefore very much welcome the NTIA's emphasis on incentivizing privacy by design and, more generally, privacy research.

We note that NTIA's approach focuses on "*the outcomes of organizational practices, rather than on dictating what those practices should be.*" In this respect, we certainly agree that data protection rules should normally not prescribe specific ways of data processing but rather ensure that such processing complies with certain principles and respects certain safeguards. In addition, in our experience a high level of data protection can be applied in a flexible way by making available **different tools to address the broad variety of processing operations** that characterizes the digital economy. This can be achieved by providing for different legal grounds that can be relied upon to collect and process data (not just consent, but also for instance the performance of a contract or legitimate interests of the business operator or third parties). Similar considerations apply for international data transfers: while they should not undermine the level of protection "at home", different instruments can be developed to facilitate such data transfers. In a system based on accountability, this may include elements of co-regulation such as codes of conduct and certification that are 'bottom-up' and can help companies to demonstrate compliance in a way that is adapted to the specific needs and features of their sector or business model.

We also agree on the usefulness of a "**risk-based approach**", which is at the core of NTIA's proposal. As indicated in the RFC under the heading of "scalability", risks are not linked to the size of the business operator, but rather to the type of processing (e.g. volume, categories of personal data handled).

In our view, certain protections can indeed be applied in a flexible way, depending on the level of risk for privacy of the processing operations involved (distinguishing, for instance, between data processing as an ancillary activity and the large-scale processing of sensitive data). In this way, processing operations with limited impact on privacy could be subject to a reduced regulatory burden, thereby also creating incentives to develop innovative, privacy-friendly solutions from the earliest stages of development. However, as privacy is a fundamental value, a certain 'baseline' protection should be ensured regardless of the risks involved. Therefore, we believe that risk assessments should not be applied to all privacy safeguards, but only to additional obligations for business operators beyond that 'baseline'.

More generally, it is important to ensure that "risk-based flexibility" and more generally attention to overall context do not undermine legal certainty and the possibility for both individuals (through private actions) and the competent oversight authority to enforce compliance. Likewise, while the right to privacy and data protection is of course not absolute and reasonable limitations to protect other rights or important public interests

can be justified, we believe that there is a benefit in not tying the level of protection from the outset to broad notions such as "appropriateness" and "reasonableness".

Finally, we welcome that the proposed approach also seeks to contribute to **harmonization and interoperability at global level**. In our view, this can best be achieved through increased convergence, which is, in fact, already a clear global trend as many countries in different regions of the world are putting in place data protection rules that reflect the principles set out in this submission. The same applies for a number of regional instruments, like for instance the Ibero-American Data Protection Standards, as well as the Council of Europe Convention 108[5], the only binding multinational agreement on data protection that already brings together more than 50 State Parties from around the globe. The United States is currently an observer to Convention 108 and should considerer becoming a Party, as it has done with other Council of Europe instruments (e.g. the Cybercrime Convention). Given that companies increasingly operate across borders and prefer to apply a single set of rules in all of their business operations worldwide, joining this global trend would help commercial operators navigate between different legal systems and offer new opportunities to facilitate trade.

We hope that the present observations will be useful for you and we of course stand ready to further explain or discuss these issues.

Yours sincerely,

Bruno Gencarelli
Head of Unit

[e-signed]

[5] Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 180) and 2001 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181). On 18 May 2018, the 128th Ministerial Session of the Council of Europe's Committee of Ministers adopted a Protocol (CETS No. 223) amending Convention 108. This Amending Protocol was opened for signature on 10 October 2018.

Before the
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION
Washington, DC

In the Matter of Developing the Administration's Approach to Consumer Privacy	Docket No. 180821780–8780–01

To: National Telecommunications and Information Administration
Date: November 9, 2018

I. Introduction

Thank you for the opportunity for FTC staff to comment on the Department of Commerce, National Telecommunications and Information Administration ("NTIA") Request for Comment on Developing the Administration's Approach to Consumer Privacy ("RFC").

As the nation's consumer protection and competition agency, the Federal Trade Commission ("FTC" or "Commission") is committed to protecting consumers' privacy and security interests while promoting competition and innovation. We commend the NTIA for addressing this timely issue and support efforts by both the Administration and Congress to evaluate the effectiveness of current frameworks and to identify "ways to advance consumer privacy while protecting prosperity and innovation."[1] The Commission is exploring precisely these issues through a series of Hearings on Competition and Consumer Protection in the 21st Century.[2]

[1] NAT'L TELECOMM. & INFO. ADMIN., Request for Comment on Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48600 (Sept. 26, 2018).

[2] *See* Press Release, Fed. Trade Comm'n, FTC Announces Hearings On Competition and Consumer Protection in the 21st Century (June 20, 2018), https://www ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st. Just this week, the Commission held hearings on the Intersection of Big Data, Privacy, and Competition. Agenda, The Intersection of Big Data, Privacy, and Competition, Hearings on

Consumer data privacy is an important and timely topic. Today, companies often provide digital services and content powered by (or in exchange for) consumer data. News headlines draw attention to remarkable innovation—in mobile apps,[3] mobile payment systems,[4] connected devices,[5] automated cars,[6] etc.—that both stems from and necessitates the collection, use, and disclosure of consumer data. At the same time, however, news headlines highlight potentially problematic privacy practices: a dating app's disclosure of HIV status to software vendors,[7] a tracking firm's inadvertent exposure of the real-time geolocation data of 200 million people,[8] or an IoT firm's decision to track sex toy use without users' consent.[9] These twin trends—data-driven innovation and increasing data privacy concerns—have raised important questions about the ability of the existing legal landscape to protect consumers' privacy interests. In addition, as

---

Competition and Consumer Protection in the 21st Century, Fed. Trade Comm'n (Nov. 6-8, 2018), https://www ftc.gov/system/files/documents/public_events/1418633/hearings-agenda-au_0.pdf. We will be holding additional hearings on data security and privacy in December 2018 and February 2019, respectively. Press Release, Fed. Trade Comm'n, FTC Announces Sessions on Consumer Privacy and Data Security As Part of its Hearings on Competition and Consumer Protection in the 21st Century, Oct. 26, 2018, https://www ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its. All of these hearings, as well as the public comments we have received and expect to receive in the future, serve as an opportunity for the Commission to explore the issues further and develop greater expertise.

[3] Eric Rosenbaum, *The Most Popular Free Apps to Keep You Healthy in 2018*, CNBC, Jan. 5, 2018, https://www.cnbc.com/2018/01/05/top-5-free-apps-to-keep-you-healthy-in-2018.html.

[4] Michael Muchmore, *The Best Mobile Payment Apps of 2018*, PC MAGAZINE, Apr. 2, 2018, https://www.pcmag.com/roundup/358553/the-best-mobile-payment-apps.

[5] Charlie Osborne, *The Best IoT, Smart Home Gadgets in 2018*, ZDNET, Apr. 24, 2018, https://www.zdnet.com/pictures/the-best-iot-smart-home-gadgets-in-2018/.

[6] Marco della Cava, *What's It Like to Run Errands in a Self-driving Car? Some Phoenix Regulars Are Sold on Waymo*, USA TODAY, Oct. 10, 2018, https://www.usatoday.com/story/money/2018/10/10/waymo-self-driving-cars-hit-10-million-road-miles-they-aim-public-debut/1536441002/.

[7] Natasha Singer, *Grindr Sets Off Privacy Firestorm After Sharing Users' H.I.V.-Status Data*, N.Y TIMES, Apr. 3, 2018, https://www.nytimes.com/2018/04/03/technology/grindr-sets-off-privacy-firestorm-after-sharing-users-hiv-status-data html.

[8] Brian Barrett, *A Location Sharing Disaster Shows How Exposed You Really Are*, WIRED, May 19, 2018, https://www.wired.com/story/locationsmart-securus-location-data-privacy/.

[9] Alex Hern, *Vibrator Maker Ordered to Pay Out C$4m for Tracking Users' Sexual Activity*, THE GUARDIAN, Mar. 14, 2017, https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits.

the RFC notes,[10] the emergence of new legal frameworks at the state and international levels presents the question of whether a new national approach would benefit consumers and competition.

As described below, the Commission has deep experience in protecting consumer privacy and fostering innovation. For decades, the Commission has enforced our existing consumer protection laws, which take a flexible, risk-based approach to consumer privacy that "balance[s] business needs, consumer expectations, legal obligations, and potential privacy harms, among other inputs."[11] In this comment, we first describe our experience in protecting consumers' privacy interests through enforcement, education, and policy work. We then discuss the guiding principles of our current approach: balancing risk of harm with the benefits of innovation and competition. After laying this groundwork, the comment applies this approach of balancing risks and benefits to address four specific areas highlighted in the RFC: security, transparency, control, and FTC enforcement. Finally, the comment looks to the future, considering potential directions for privacy policy in the United States.

II. Background on the FTC

The FTC is an independent administrative agency responsible for protecting consumers and promoting competition. The Commission has proven itself a government leader in privacy, through enforcement actions, consumer and business education, and policy efforts.

On the enforcement front, the FTC conducts investigations and brings cases under a wide range of laws. First and foremost, the Commission enforces the FTC Act, which prohibits unfair and deceptive acts or practices—including unfair and deceptive privacy and security practices—

[10] RFC, *supra* note 1 at 48600.

[11] *Id.* at 48602.

in or affecting commerce.[12] The FTC enforces specific statutes that protect a host of consumer data, including certain health information (via the Health Breach Notification Rule),[13] credit information (through the Fair Credit Reporting Act ("FCRA")),[14] financial data (as described in the privacy and security rules implementing the Gramm-Leach-Bliley ("GLB") Act),[15] and children's information (as defined in the Children's Online Privacy Protection Act ("COPPA")).[16] The Commission also enforces laws that protect consumers from certain intrusions, such as unwanted phone calls or emails, including the Telemarketing Sales Rule ("TSR"),[17] CAN-SPAM Rule,[18] and the Fair Debt Collection Practices Act ("FDCPA").[19]

[12] 15 U.S.C. § 45(a). The FTC's unfairness cases have challenged privacy and security practices that cause or are likely to cause substantial harm to consumers. *See, e.g.*, Aaron's, Inc., No. C-442 (F.T.C. Mar. 10, 2014), https://www ftc.gov/system/files/documents/cases/140311aaronscmpt.pdf (Complaint); FTC v. Ruby Corp. No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016), https://www ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf (Complaint). And, when businesses present otherwise beneficial products and services in a deceptive manner, consumers lose the opportunity to make informed choices and may be injured. *See, e.g.*, Practice Fusion, Inc., No. C-4591 (F.T.C. Aug. 15, 2016), https://www ftc.gov/system/files/documents/cases/160816practicefusioncmpt.pdf (Complaint) (alleging that the company deceived consumers about why it was collecting potentially sensitive healthcare information); FTC v. Vizio, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), https://www ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf (Complaint) (Smart TV manufacturer Vizio offered consumers an innovative TV, but allegedly misled consumers about the extent to which Vizio's TVs collected and used consumer viewing information).

[13] 16 C.F.R. Part 318.

[14] 15 U.S.C. § 1681 *et seq*.

[15] 15 U.S.C. § 6801 *et seq*.; Privacy of Consumer Financial Information, 16 C.F.R. Part 313 ("GLB Privacy Rule"); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("GLB Safeguards Rule").

[16] 15 U.S.C. § 6501 *et seq*. and Children's Online Privacy Protection Rule, 16 C.F.R. Part 312 ("COPPA Rule").

[17] Telemarketing Sales Rule, 16 C.F.R. Part 310, implementing Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 *et seq*.

[18] CAN-SPAM Rule, 16 C.F.R. Part 316, implementing Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM") of 2003, 15 U.S.C. § 7701 *et seq*.

[19] 15 U.S.C. § 1692 *et seq*.

The FTC has brought hundreds of cases protecting the privacy and security of consumer information—both on and offline—held by companies large and small.[20] FTC enforcement actions have addressed a variety of illegal privacy and security practices, such as:

- collecting information from children online without parental consent;[21]
- deceiving consumers about collection, use, and/or disclosure of their financial, health, video, or other personal information;[22]
- making false promises about compliance with the EU-U.S. Privacy Shield (and the predecessor U.S.-EU Safe Harbor);[23]
- deceptively tracking consumers online;[24]
- disclosing highly sensitive, private consumer data to unauthorized third parties;[25]

---

[20] Letter from Edith Ramirez, Chairwoman, Fed Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality, European Commission, at 3 (Feb. 23, 2016), https://www.ftc.gov/public-statements/2016/02/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice.

[21] United States v. VTech Elec. Ltd., No. 1:18-cv-114 (N.D. Ill. Jan. 8, 2018), https://www ftc.gov/system/files/documents/cases/vtech_file_stamped_stip_order_1-8-18.pdf (Stipulated Order).

[22] *See, e.g.*, PayPal, Inc., No. C-4651 (F.T.C. May 23, 2018), https://www ftc.gov/system/files/documents/cases/1623102-c4651_paypal_venmo_decision_and_order_final_5-24-18.pdf (Decision and Order); Practice Fusion, Inc., No. C-4591 (F.T.C. Aug. 15, 2016), https://www ftc.gov/system/files/documents/cases/160816practicefusiondo.pdf (Decision and Order); FTC v. Vizio, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), https://www ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf (Stipulated Order); Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), https://www ftc.gov/system/files/documents/cases/141231snapchatdo.pdf (Decision and Order); *see generally* Fed. Trade Comm'n, Privacy and Security Cases, https://www ftc.gov/datasecurity (last visited Nov. 5, 2018).

[23] Decusoft, LLC, No. C-4630 (F.T.C. Nov. 20, 2017), https://www ftc.gov/system/files/documents/cases/1723173_c4630_decusoft_decision_and_order_11-29-17.pdf (Decision and Order); Tru, Comm., Inc., No. C-4628 (F.T.C. Nov. 20, 2017), https://www ftc.gov/system/files/documents/cases/1723171_c4628_tru_communication_decision_and_order_11-29-17.pdf (Decision and Order); Md7, LLC, No. C-4629 (F.T.C. Nov. 20, 2017), https://www ftc.gov/system/files/documents/cases/1723172_c4629_md7_decision_and_order_11-29-17.pdf (Decision and Order); ReadyTech Corp., No. 1823100 (F.T.C. July 2, 2018), https://www ftc.gov/system/files/documents/cases/1823100_readytech_corp_decision_and_order_7-2-18.pdf (Decision and Order).

[24] *See, e.g.*, Compete, Inc., No. C-4384 (F.T.C. Feb. 20, 2013), https://www ftc.gov/enforcement/cases-proceedings/102-3116/compete-inc (Decision and Order); Upromise, Inc., No. C-4351 (F.T.C. Mar. 27, 2012), https://www ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc (Decision and Order); Sears Holding Mgt. Corp., No. C-4264 (F.T.C. Aug. 31, 2009), https://www ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter (Decision and Order).

[25] *See, e.g.*, FTC v. Accusearch, Inc., 570 F.3d 1187, 1195 (10th Cir. 2009).

- publicly posting private data online without consumers' knowledge or consent;[26]
- installing spyware or other malware on consumers' computers;[27]
- failing to provide reasonable security for consumer data, including children's information;[28]
- spamming and defrauding consumers;[29]
- making harassing calls about phantom debt and leaving threatening voicemails about debt collection;[30]
- failing to comply with legal requirements when generating automated data used to deny housing to applicants;[31] and
- violating Do Not Call and other telemarketing rules.[32]

These enforcement actions send an important message: the FTC holds companies accountable for their information practices.

---

[26] *See, e.g.*, Jerk, LLC, No. 9361 (F.T.C. Apr. 2, 2014), https://www ftc.gov/system/files/documents/cases/140407jerkpart3cmpt.pdf (Complaint); Craig Brittain, No. C-4564 (F.T.C. Dec. 28, 2015), https://www.ftc.gov/system/files/documents/cases/160108craigbrittaindo.pdf (Decision and Order).

[27] *See generally*, Fed. Trade Comm'n, Spyware and Malware, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware (last visited Nov. 5, 2018).

[28] *See, e.g.*, Accretive Health, Inc., No. C-4432 (F.T.C. Feb. 24, 2014), https://www ftc.gov/system/files/documents/cases/140224accretivehealthdo.pdf (Decision and Order); FTC v. Neovi Inc., 604 F.3d 1150 (9th Cir. 2010); *see generally* FTC Privacy and Security Cases, *supra* note 22.

[29] *See, e.g.*, CPATank, Inc., No. 1:14-cv-01239 (N.D. Ill. Feb. 25, 2014), https://www ftc.gov/system/files/documents/cases/140228cpatankorder.pdf (Stipulated Final Judgment); FTC v. INC21.com Corp., 688 F. Supp. 2d 927 (N.D. Cal. 2010), *aff'd*, 475 Fed. Appx. 106 (9th Cir. 2012); *see generally* Fed. Trade Comm'n, Online Advertising and Marketing, https://www ftc.gov/tips-advice/business-center/advertising-and-marketing/online-advertising-and-marketing (last visited Nov. 5, 2018).

[30] FTC v. Global Processing Solutions, LLC, No. 1:17-cv-04192-MHC (N.D. Ga. July 17, 2018), https://www ftc.gov/system/files/documents/cases/advanced_mediation_group_stip_order_re_snow_redacted.pdf (Stipulated Order).

[31] RealPage, Inc., No. 3:18-cv-02737-N (N.D. Tex. Oct. 16, 2018), https://www ftc.gov/system/files/documents/cases/152_3059_realpage_inc_stipulated_order_10-16-18.pdf (Stipulated Order).

[32] *See, e.g.*, FTC. v. Christiano, No. SA CV 18-0936, (C.D. Cal. May 31, 2018) https://www ftc.gov/system/files/documents/cases/netdotsolutions_complaint.pdf (Complaint); Credit Protection Ass'n, No. 3:16-cv-01255-D (N.D. Tex. May 9, 2016), https://www ftc.gov/system/files/documents/cases/160509cpaorder.pdf (Stipulated Final Order); FTC v. E.M.A. Nationwide, Inc., 767 F.3d 611 (6th Cir. 2014).

The FTC also engages in consumer and business education to increase the impact of its enforcement actions. The FTC uses a variety of tools—such as blogging, distributing educational materials, and connecting through social media—to educate consumers and businesses on a wide range of topics. Recent topics have included information security,[33] credit freezes,[34] mobile apps and health data,[35] geolocation and children's privacy,[36] and the privacy of genetic information.[37]

Finally, the FTC has undertaken numerous policy initiatives designed to promote the privacy and security of consumer data. Workshops have delved into technology-specific topics, such as connected cars,[38] education technology,[39] drones,[40] and smart TVs.[41] The Commission has issued reports that address timely issues, such as facial recognition technology,[42] the data

---

[33] Fed. Trade Comm'n, Cybersecurity for Small Business, FTC Business Center, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity (last visited Nov. 5, 2018); Thomas B. Pahl, Stick With Security, FTC Business Blog (Sept. 22, 2017, 11:32 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/09/stick-security-put-procedures-place-keep-your-security.

[34] Fed. Trade Comm'n, Credit Freeze FAQs, https://www.consumer ftc.gov/articles/0497-credit-freeze-faqs (last visited Nov. 5, 2018).

[35] Fed. Trade Comm'n, Mobile Health Apps Interactive Tool (Apr. 2016), https://www ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[36] Press Release, Fed. Trade Comm'n, FTC Warns Gator Group, Tinitell that Online Services Might Violate COPPA, Apr. 27, 2018, https://www.ftc.gov/news-events/press-releases/2018/04/ftc-warns-gator-group-tinitell-online-services-might-violate.

[37] Lesley Fair, DNA Test Kits: Consider the Privacy Implications, FTC Consumer Information Blog, Dec. 12, 2017, ttps://www.consumer ftc.gov/blog/2017/12/dna-test-kits-consider-privacy-implications.

[38] Event Announcement, Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles, Fed. Trade Comm'n (June 28, 2017), https://www ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.

[39] Event Announcement, Student Privacy and Ed. Tech., Fed. Trade Comm'n (Dec. 1, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech.

[40] Event Announcement, Fall Technology Series: Drones, Fed. Trade Comm'n (Oct. 13, 2016), https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones.

[41] Event Announcement, Fall Technology Series: Smart TV, Fed. Trade Comm'n (Dec. 7, 2016), https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv.

[42] FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (Oct. 2012), https://www ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

broker industry,[43] and the privacy and security implications of the Internet of Things.[44] Currently, the Commission is holding a series of Hearings on Competition and Consumer Protection in the 21st Century, which will include hearings focused specifically on privacy and data security.[45]

III. Guiding Principles

The FTC supports a balanced approach to privacy that weighs the risks of data misuse with the benefits of data to innovation and competition. Striking this balance correctly is essential to protecting consumers and promoting competition and innovation, both within the U.S. and globally. The FTC has brought cases under various statutes addressing privacy-related harms that fall into at least four categories:

- **Financial Injury:** Financial injury can manifest in a variety of ways: fraudulent charges, delayed benefits, expended time, opportunity costs, fraud, and identity theft, among other things.[46]

- **Physical Injury:** Physical injuries include risks to individuals' health or safety, including the risks of stalking and harassment.[47] Physical safety concerns also helped to drive Congress's enactment of COPPA in 1998.[48]

---

[43] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), https://www ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[44] *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Jan. 2015), https://www ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (Staff Report); *see also* Event Announcement, Internet of Things: Privacy and Security in a Connected World, Fed. Trade Comm'n (Nov. 19, 2013), https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[45] Press Release on FTC Hearings, *supra* note 2.

[46] *See, e.g.*, TaxSlayer, LLC, No. C-4626 (F.T.C. Oct. 20, 2017), https://www ftc.gov/system/files/documents/cases/1623063_c4626_taxslayer_complaint.pdf (Complaint) (alleging delayed benefits, expended time, risk of identity theft).

[47] *See* FTC v. Accusearch, Inc., No. 06-CV-0105 (D. Wyo. May 3, 2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf (Complaint) (alleging that telephone records pretexting endangered consumers' health and safety); FTC v. EMP Media, Inc., No. 2:18-cv-00035 (D. Nev. Jan. 9, 2018) https://www ftc.gov/system/files/documents/cases/1623052_myex_complaint_1-9-18.pdf (Complaint) (alleging revenge porn website led to threats and harassment against individuals depicted).

- **Reputational Injury:** Reputational injury involves disclosure of private facts about an individual that damages the individual's reputation. Tort law recognizes reputational injury.[49] The FTC has brought cases involving this type of injury, for example, in a case involving public disclosure of individuals' Prozac use[50] and public disclosure of individuals' membership on an infidelity-promoting website.[51] Participants in the FTC's December 2017 workshop on informational injury elaborated on the reputational injury (among other harms) that can result from disclosure of private data.[52]

- **Unwanted Intrusion:** Unwanted intrusions involve two categories. The first includes activities that intrude on the sanctity of people's homes and their intimate lives. The FTC's cases involving a revenge porn website, an adult-dating website, and companies spying on people in their bedrooms through remotely-activated webcams fall into this category.[53] The second category involves unwanted commercial intrusions, such as telemarketing, spam, and harassing debt collection calls. As noted above, the FTC enforces laws addressing each of these categories of harm.

In addition to considering the risks identified above, any approach to privacy must also consider how consumer data fuels innovation and competition. The digital economy has benefitted consumers in many ways, saving individuals' time and money, creating new opportunities, and conferring broad social and environmental benefits. For example, recent innovations have enabled:

---

[48] *See* COPPA Legislative History, 105th Congress, 2nd Session, Vol. 144 (Oct. 21, 1998), https://www.congress.gov/congressional-record/1998/10/21/senate-section/article/S12741-4.

[49] Under the tort of public disclosure of private facts (or publicity given to private life), a plaintiff may recover where the defendant's conduct is highly offensive to a reasonable person. Restat. 2d of Torts, § 652D (1977).

[50] Eli Lilly and Co., No. 4047 (F.T.C. May 8, 2002), https://www ftc.gov/sites/default/files/documents/cases/2002/05/elililly do htm (Decision and Order).

[51] FTC v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016), https://www ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf (Complaint).

[52] Transcript, Informational Injury Workshop, Fed. Trade Comm'n (Dec. 12, 2017), https://www ftc.gov/system/files/documents/public_events/1256463/informational_injury_workshop_transcript_with_index_12-2017.pdf (citing "doxing," the practice of deliberately releasing private information to encourage harassment, and relaying information about shaming, harassment, and discrimination after disclosure of individuals' HIV status); FTC INFORMATIONAL INJURY WORKSHOP: BE AND BCP STAFF PERSPECTIVE, FED. TRADE COMM'N (Oct. 2018), https://www ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

[53] *See* Press Release, FTC Halts Computer Spying, Fed. Trade Comm'n, Sept. 25, 2012, https://www ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying. *See also* Aaron's, Inc., No. C-442 (F.T.C. Mar. 10, 2014), https://www ftc.gov/system/files/documents/cases/140311aaronsdo.pdf (Decision and Order) (similar case involving similar software).

- Better predictions about and planning for severe weather events, including updated flood warnings, real-time evacuation routes, and improved emergency responses and measures, that can allow people to plan for and avoid dangerous conditions.[54]

- Improved consumer fraud detection in the financial and banking sector, as institutions can obtain insights into consumers' purchasing and behavior patterns that will allow them to proactively identify and immediately stop fraudulent transactions when they are discovered. [55]

- Free or substantially discounted services, including free communications technologies (email, VoIP, etc.), inexpensive and widely available financial products, and low-cost entertainment.

- Safer, more comfortable homes, as IoT devices detect flooding in basements, monitor energy use, identify maintenance issues, and remotely control devices such as lights and ovens.[56]

- Better health and wellness, as a variety of diagnostics, screening apps, and wearables enable richer health inputs, remote diagnosis by medical professionals, and virtual consultations.[57]

- More convenient shopping, as retail stores track both sales and inventory in real-time via shopping data to optimize product inventory in each store.[58]

---

[54] *See, e.g.*, Ali McConnon, *AI Helps Cities Predict Natural Disasters*, WALL ST. J., June 26, 2018, https://www.wsj.com/articles/ai-helps-cities-predict-natural-disasters-1530065100; *New Research Leverages Big Data to Predict Severe Weather*, SCIENCE DAILY, June 21, 2017, https://www.sciencedaily.com/releases/2017/06/170621145133.htm; Mark Puleo, *Esri Mapping, Waze Partner to Aid Emergency Responders, Residents Navigate amid Hurricane Florence*, ACCUWEATHER, Sept. 14, 2018, https://www.accuweather.com/en/weather-news/esri-mapping-waze-partner-to-aid-emergency-responders-residents-navigate-amid-hurricane-florence/70006063.

[55] *See* Mark Labbe, *Credit Card Giants Step Up AI Fraud Detection*, TECHTARGET, Sept. 20, 2018, https://searchenterpriseai.techtarget.com/news/252449044/Credit-card-giants-step-up-AI-fraud-detection; *MIT Researchers Use Machine Learning for Credit Card Fraud Detection*, INNOVATION ENTERPRISE CHANNEL, Sept. 24, 2018, https://channels.theinnovationenterprise.com/articles/mit-researchers-use-machine-learning-for-credit-card-fraud-detection.

[56] *See generally* INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 44 at 8-9; *A Smarter World: How AI, The IoT And 5G Will Make All The Difference*, FORBES, Sept. 21, 2018, https://www forbes.com/sites/intelai/2018/09/21/a-smarter-world-how-ai-the-iot-and-5g-will-make-all-the-difference/.

[57] Peter H. Diamandis, *Three Huge Ways Tech Is Overhauling Healthcare*, SINGULARITY HUB, July 6, 2018, https://singularityhub.com/2018/07/06/three-huge-ways-tech-is-overhauling-healthcare/. Indeed, "[d]espite patient privacy risks that collecting health data on . . . wearable devices could pose, the number of U.S. consumers tracking their health data with wearables has more than doubled since 2013 . . . ." Fred Donovan, *Despite Patient Privacy Risks, More People Use Wearables for Health*, HEALTH IT SECURITY, Oct. 1, 2018, https://healthitsecurity.com/news/despite-patient-privacy-risks-more-people-use-wearables-for-health.

- More relevant online experiences, as retailers provide customized offers and video services recommend new shows.

- Easier-to-find parking, as cities deploy smart sensors to provide residents with real-time data about available parking spots.[59]

- Increased connectivity, as consumers can get immediate answers to questions by asking their digital voice assistants and can remotely operate devices, such as lights and door locks, with a voice command or single touch on a phone.[60]

Privacy standards that give short shrift to the benefits of data-driven practices may negatively affect innovation and competition. Moreover, regulation can unreasonably impede market entry or expansion by existing companies; the benefits of privacy regulation should be weighed against these potential costs to competition.[61]

The FTC is uniquely situated to balance consumers' interests in privacy, innovation, and competition for four reasons. First, a risk-based approach is in the FTC's institutional DNA. The FTC Act prohibits unfair or deceptive acts or practices; Congress defined "unfair" acts or practices as those in which consumer harm outweighs the benefits.[62] In other words, according

---

[58] *See* Bernard Marr, *The Brilliant Ways Kimberly-Clark Uses Big Data, IoT & Artificial Intelligence To Boost Performance*, FORBES, July 13, 2018, https://www.forbes.com/sites/bernardmarr/2018/07/13/the-brilliant-ways-kimberly-clark-uses-big-data-iot-artificial-intelligence-to-boost-performance/#23eda32c36d7.

[59] *See* Teena Maddox, *Big Data Takes a Big Leap in Kansas City with Smart Sensor Info on Parking and Traffic*, TECH REPUBLIC, Apr. 20, 2017, https://www.techrepublic.com/article/big-data-takes-a-big-leap-in-kansas-city-with-smart-sensor-info-on-parking-and-traffic/.

[60] Forbes Agency Council, *How Voice Technology Is Changing The Way We Work*, FORBES, July 27, 2018, https://www forbes.com/sites/forbesagencycouncil/2018/07/27/how-voice-technology-is-changing-the-way-we-work/#3d4894bc4a4d; Marc Zao-Sanders, *The Productivity Booster You Have in Your Pocket, But Probably Don't Use*, HARV. BUS. REV., July 19, 2018, https://hbr.org/2018/07/the-productivity-booster-you-have-in-your-pocket-but-probably-dont-use.

[61] Consider, for example, a small outdoor equipment company trying to expand its customer base. Under current law, the company can use targeted ads to reach consumers who have browsed online for hiking equipment or national park passes. Without the ability to serve these data-driven ads, it would be difficult for the company to insert itself into a market dominated by large, well-entrenched players. The resulting lack of competition could hurt consumers, giving them fewer and more expensive choices.

[62] Fed. Trade Comm'n, Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction, 104 F.T.C. 1070, 1071 (1984) (*appended to* Int'l Harvester Co., 104 F.T.C. 949 (1984)); Section 15 U.S.C. § 45(n) ("The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not

to the FTC's enabling statute, the FTC is *required* to perform a cost-benefit analysis before finding a practice is unfair.[63] Second, the FTC is the only U.S. federal agency with both competition and consumer protection jurisdiction. Thanks to this dual expertise, the FTC has a rich understanding of the benefits and costs to consumers of restricting commercial data flows. Third, the Commission has demonstrated its ability to conduct rulemaking to safeguard consumer privacy and security and provide guidance to businesses. For example, the Commission responded to the Congressional mandate to issue rules on children's and financial privacy by issuing the COPPA Rule,[64] the GLB Privacy Rule,[65] and the GLB Safeguards Rule.[66] Finally, the FTC has the institutional expertise: in addition to the litigating staff who have brought the agency's enforcement actions in privacy and data security, its Bureau of Economics has more than 75 economists who provide independent policy advice to the Commission on both competition and consumer protection matters. The Commission has used these and other tools to balance consumers' privacy interests with business' need for flexibility since the inception of its privacy program over 20 years ago.

IV. The FTC's Comments on Topics Identified in the NTIA's Request for Comment

We offer our observations in four areas: security, transparency, choice, and FTC enforcement. We note that although the RFC encompasses a wide range of social, political, and economic goals, our comments focus on discrete items related to ensuring that markets work for consumers by preventing unfair, deceptive, and anticompetitive conduct.

---

reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

[63] Of course, the FTC also challenges deceptive practices, which does not involve an explicit cost-benefit analysis. 15 U.S.C. § 45(a).

[64] 16 C.F.R. Part 412, *supra* note 16.

[65] 16 C.F.R. Part 313, *supra* note15.

[66] 16 C.F.R. Part 314, *supra* note 15.

A. Security

The FTC has been very active in data security, bringing over 60 cases alleging that companies did not maintain reasonable security. The FTC has taken enforcement action when it has determined that data security is inadequate or disclosures about data security are misleading.[67] The Commission has long issued calls for comprehensive data security legislation, so as to obtain additional tools.[68] The Commission is also exploring its remedial authority during the upcoming hearings relating to data privacy.[69]

B. Transparency

Transparency is another longstanding privacy tenet championed by the FTC.[70] The challenge is *how* and *when* to be transparent—how and when to provide important information about data collection and use in a way that it is accessible and meaningful to consumers.[71] The

---

[67] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2017, at 4-5 (Jan. 2018), https://www ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives.

[68] *Id.*

[69] *See supra* note 2.

[70] *See, e.g.*, FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (Staff Report).

[71] Consistent with observed consumer behavior, some surveys suggest that consumers are willing to share their information with companies to personalize experiences as long as companies are transparent about their information practices. *See* John Hall, *What You Should Know About Privacy That Will Help Consumers Trust Your Brand*, FORBES, Apr. 4, 2018, https://www forbes.com/sites/johnhall/2018/04/25/what-you-should-know-about-privacy-that-will-help-consumers-trust-your-brand/#472a4bf3135a (describing research). In other surveys, respondents report a willingness to leave brands that use their personal data without their knowledge. *See* Kevin Cochrane, *To Regain Consumers' Trust, Marketers Need Transparent Data Practices*, HARV. BUS. REV., June 13, 2018, https://hbr.org/2018/06/to-regain-consumers-trust-marketers-need-transparent-data-practices (describing research showing that 79% of consumers will leave a brand if their personal data is used without their knowledge).

Although consumers report placing a high value on transparency, some empirical studies raise questions about whether consumers, in fact, want more information when making decisions. *See, e.g.*, Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton Univ. Press 2014) (arguing that consumers make choices by stripping information away).

This disconnect between consumers' stated and revealed preferences is an example of the so-called "privacy paradox." *See, e.g.*, Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, SCIENCE 347 (6221), 509-514 (2015) (describing privacy paradox and potential explanations).

RFC rightfully notes that the hallmarks of many current privacy policies (which are typical of efforts to respond to calls for transparency) are not salutary: many are characterized by their bloat, opacity, and legalese.[72] Despite these weaknesses, privacy policies and other disclosures do provide accountability.[73] Within an organization, drafting privacy policies helps companies understand their information practices. Outside the organization, the disclosures give interested consumers more information. They also give the press, advocacy organizations, and regulators information about the company's practices, enabling them to expose problematic practices, and helping regulators to hold companies to their promises.[74]

To retain the accountability-promoting benefits of transparency, while minimizing reliance on long, dense privacy policies, a more consumer-oriented approach would address the context, form, and effectiveness of disclosures, and be based on consumer demand for information.[75] The Commission has long been a proponent of context-specific disclosures, at the point at which consumers are making decisions about their data, which could take the form of set-up wizards, dashboards, or other in-line notices.[76] The Commission has also encouraged sector-specific model privacy notices that are clear, conspicuous, and succinct.[77] The FTC could

---

[72] RFC, *supra* note 1 at 48601.

[73] *See, e.g.*, Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044 (2017).

[74] *Id.* at 1045 (describing how well-drafted privacy statements "create organizational accountability," inform "highly motivated individuals," and enable "those who act on behalf of consumers . . . [to] ask the hard questions . . . [,] raise public awareness and create consequences when an organization has inadequate or problematic privacy practices").

[75] *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, at i (Mar. 2012), https://www ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[76] *See, e.g.*, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, supra note 44 at 25-26.

[77] *See, e.g.*, Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62890, 62891 (Dec. 1, 2009) (setting forth the requirements of a model privacy notice). Staff continues to encourage more research about consumer demand for, understanding of, and use of this kind of disclosure. *See, e.g.*, Event Announcement, Putting Disclosures to the Test, Fed. Trade Comm'n (Sept. 15, 2016), https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.

promote accountability under an improved disclosure regime through the exercise of its authority to challenge deceptive disclosures.

C. Control

The FTC has long encouraged a balanced approach to control. Giving consumers the ability to exercise meaningful control over the collection and use of data about them is beneficial in some cases.[78] However, certain controls can be costly to implement and may have unintended consequences. For example, if consumers were opted out of online advertisements by default (with the choice of opting in), the likely result would include the loss of advertising-funded online content.[79]

The proper approach to consumer control—one that balances costs and benefits—takes consumer preferences, context (including risk), and form into account. First, whether choice is necessary depends on the context. If the data use matches the context of the transaction or the company's relationship with the consumer, or is required or authorized by law, choice may be presumed or choice may not be necessary. For example:

- **Product and service fulfillment:** Retailers disclose consumers' contact information to delivery companies that ship their purchases. A connected thermostat collects consumers' temperature preferences to provide automated services.
- **Internal operations:** Hotels and restaurants collect customer satisfaction surveys. Websites collect click-through rates to improve site navigation.
- **Fraud prevention:** Retailers check drivers' licenses at the point of sale to prevent fraud. Online businesses scan ordinary web server logs to detect fraud. Stores use video cameras to spot theft.

---

[78] *See, e.g.*, Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861 (2000) (discussing longstanding conception of privacy as control over one's data).

[79] Interactive Survey of U.S. Adults, DIGITAL ADVERTISING ALLIANCE, Apr. 2013, http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf (reporting that 92% of respondents agreed that free content is important to the value of the Internet).

- **Legal compliance and public purpose:** Search engines disclose customer data in response to legal process. A business reports a consumer's delinquent account to a credit bureau.

- **First-party marketing:** Retailers recommend products based upon consumers' prior purchases and collect data for loyalty programs.[80]

Choice also may be unnecessary when companies collect and disclose de-identified data,[81] which can power data analytics and research (potentially benefiting consumers and society), while minimizing privacy concerns. For example, consumer appliance companies can collect data about smart device usage in homes, publicize usage data in aggregate form, and encourage energy savings in households. Medical researchers can collect data from wearable devices in de-identified form to improve health outcomes for a larger patient population.

By contrast, choice is important when the risk of harm might significantly increase, such as where the data is sensitive (as in cases involving information about children, financial and health information, and Social Security numbers). Consumers should also be given a choice when a company uses the data in a manner inconsistent with its original representations. For example, the FTC brought an action against Gateway Learning, a vendor of children's educational products, when the company disclosed information about children to marketers despite the fact that the privacy policy in place at the time of the data's collection stated the

[80] Providing choices in some of these contexts may have negative effects. For example, consumers inundated by obvious or seemingly insignificant choices may become less attentive to choices that are important to them. Likewise, offering choices in some instances may undermine social benefits. Bart P. Knijnenburg, Simplifying Privacy Decisions: Towards Interactive and Adaptive Solutions, Decisions@RecSys 2013: 40-41; Sheena S. Iyengar & Mark R. Lepper, *When Choice Is Demotivating: Can One Desire Too Much of a Good Thing?*, J. OF PERSONALITY & SOC. PSYCHOL. 79, 6 (2000), 995–1006, https://faculty.washington.edu/jdb/345/345%20Articles/Iyengar%20%26%20Lepper%20(2000).pdf. For example, people who refuse to pay their bills should not be able to opt out of having that information included in credit reports, to the detriment of future creditors.

[81] A key caveat, however, is that data must be effectively de-identified, and any company that is using de-identified data should take sufficient steps to ensure that it cannot be reasonably re-identified. *See* PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 75 at 21.

company would not share such information.[82] Similarly, the Commission has charged companies with violations of Section 5 when they allegedly collected certain sensitive information in contravention of privacy policies or otherwise without adequate consumer notice.[83]

When offering choice, companies should consider the context in which the consumer actually makes the choice and design the choice mechanism to fit that context. For example, the FTC staff's report on the Internet of Things cites to innovative ways in which companies are offering these just-in-time choices, including through set-up wizards for devices, privacy "dashboards" or "command centers" that consumers can revisit at any time, or video or in-store tutorials that take place at the point of sale.[84] Some websites and apps have adopted similar mechanisms for providing just-in-time choices about, for example, online behavioral advertising.[85] Some platforms have developed browser-based tools for web surfing that give consumers control over collection of sensitive information (such as geolocation) on an app-by-

[82] Gateway Learning Corp., No. C-4120 (F.T.C. Sept. 10, 2004), https://www ftc.gov/sites/default/files/documents/cases/2004/09/040917do0423047.pdf (Decision and Order).

[83] *See, e.g.*, Blu Products, Inc., No. C-4657 (F.T.C. Sept. 6, 2018), https://www ftc.gov/system/files/documents/cases/172_3025_c4657_blu_decision_and_order_9-10-18.pdf (Decision and Order) (alleging that a mobile phone manufacturer collected contents of text messages and real-time location information despite having promised purchasers to limit data collection to what was needed to provide services); Goldenshores Tech., LLC, No. C-4446 (F.T.C. Mar. 31, 2014), https://www ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf (Decision and Order) (alleging that the privacy policy of the Android flashlight app developer deceptively failed to disclose that the app transmitted users' precise location and unique device identifier to third parties, including advertising networks); Designerware, LLC, No. C-4390 (F.T.C. Apr. 11, 2013), https://www ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwaredo.pdf (Decision and Order) (alleging that the company designed software to collect the computer's location and created a "Detective Mode" that could log computer keystrokes, take photos of anything within the web cam's view, and capture screen shots of users' activities, all without notice to the computer user).

[84] INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, *supra* note 44 at 25-26.

[85] *See, e.g.*, What Control Do I Have?, TRUSTARC, https://www.trustarc.com/consumer-privacy/about-oba/#&panel1-2 (last visited Nov. 5, 2018).

app basis.[86] Tools in some app settings allow users to exercise choices about the ads they receive.[87] These innovations may lead to choices that are more consistent with consumer preferences and risk.

D. FTC Enforcement

As discussed above, the FTC has used its enforcement authority vigorously to combat harms and the likelihood of harm from misuse of consumer data and failures adequately to secure sensitive information. Given the agency's leadership and expertise on privacy and security issues, the FTC should continue to be the primary enforcer of laws related to information flows in markets, whether under the existing privacy and security framework or under a new framework. If given additional authority in this area, the Commission may require resources commensurate with exercising that authority.

While the FTC has enforced Congress's risk-based approach, this approach is not without limitations. First, the Commission lacks authority over non-profits and common carrier activity,[88] even though the acts or practices of these market participants often have serious implications for data security.[89] In addition, under the FTC Act the FTC lacks civil penalty authority, reducing the Commission's deterrent capability.[90] Finally, the FTC lacks broad

---

[86] Jacob Kastrenakes, *How to Increase Your Privacy Online*, THE VERGE, June 7, 2018, https://www.theverge.com/2018/6/7/17434522/online-privacy-tools-guide-chrome-windows.

[87] *Id.*

[88] 15 U.S.C. § 45(a)(2) (exempting common carriers); *id.* § 44 (defining "corporations" covered in Section 5 to exclude non-profits).

[89] *See, e.g.*, Dan Patterson, *How Nonprofits Use Big Data to Change the World, Tech Republic*, TECH REPUBLIC, Feb. 8, 2017, https://www.techrepublic.com/article/how-nonprofits-use-big-data-to-change-the-world/ (describing importance of "big data" to non-profits' work).

[90] Prepared Statement of the Fed. Trade Comm'n, Oversight of the Federal Trade Commission, Committee on Energy and Commerce, at 6, July 18, 2018, https://www ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf.

rulemaking authority under the Administrative Procedures Act ("APA")[91] for consumer protection issues such as privacy and data security.[92]

Second, the privacy and security statutes the FTC does enforce (such as COPPA and the GLB Act) have their own limitations because they are targeted to particular privacy risks. For example, COPPA provides robust protections for information collected from children online, but it does not address *offline* data or data *about* children. Third, there are limitations to existing laws when data collection does not fit neatly within statutory definitions. For example, HIPAA protects health information collected by doctors' offices, insurance companies, hospitals, and a limited set of other entities, but the law does not apply to entities such as health apps, websites, data brokers, or ad networks that collect identical data directly from consumers. Although Section 5, state statutes, and common law torts may address many of these limitations, this approach likely creates uncertainty for regulated entities and uneven levels of protection for consumers.

Concerns about the limitations of current law must be balanced against the need to preserve flexibility to address complex and evolving issues related to consumer privacy and data collection, and broader impacts on innovation and competition. As noted above, these issues are the subject of the Commission's ongoing hearings.

V. The Future of U.S. Privacy Policymaking

As we look to the future of privacy policymaking in the United States, the FTC brings an unwavering commitment to protecting consumers' privacy while promoting competition and

[91] 5 U.S.C. § 500 *et seq*.

[92] Prepared Statement of the Fed. Trade Comm'n, *supra* note 67 at 6. The Commission has been granted APA rulemaking authority for discrete topics such as children's privacy, financial data security, and certain provisions of credit reporting.

innovation. Pursuant to the existing risk-based scheme, the FTC will continue to use Section 5 to police deceptive and unfair conduct to address new consumer protection issues as they arise, as well as the specific statutes it enforces to protect consumer privacy.[93]

Where companies participate in voluntary codes of conduct, the FTC has held and will continue to hold those companies accountable for the promises they make. For example, the FTC has brought more than 45 cases against companies that failed to abide by their promises to adhere to the EU-U.S. Privacy Shield or its predecessor program.[94] Similarly, when Google allegedly did not fulfill its promises to follow the Network Advertising Initiative's Self-Regulatory Code of Conduct, the FTC filed suit.[95]

Data security concerns are an important part of the privacy debate and, in light of the issues described above, the FTC continues its longstanding call that Congress consider enacting legislation that clarifies the FTC's authority and the rules relating to data security and breach notification. The FTC also understands that both Congress and the Administration are considering federal privacy legislation, and the Commission strongly supports those efforts. Any legislation should balance consumers' legitimate concerns about the protections afforded to the collection, use, and sharing of their data with business' need for clear rules of the road, consumers' demand for data-driven products and services, and the importance of flexible frameworks that foster innovation. Should Congress decide to pursue such legislation or

---

[93] *See supra* discussion at 4.

[94] *See, e.g.*, *supra* note 23 (collecting cases); *see also* Comment Filed by Director of Bureau of Consumer Protection Jessica Rich on Privacy Enforcement Implications of FCC's Proposed Set-Top Box Rulemaking, FED. TRADE COMM'N, at 4 (Apr. 22, 2016), https://www ftc.gov/system/files/documents/advocacy_documents/comment-filed-jessica-rich-privacy-enforcement-implications-fccs-proposed-set-top-box-rulemaking/160422fccsettopltr.pdf (describing cases under the U.S.-EU Safe Harbor Framework); PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 75 at 14 (noting that the FTC could enforce against companies that "fail[] to abide by the self-regulatory programs they join.").

[95] United States v. Google, Inc., 5:12-cv-04177-HRL (N.D. Cal. Aug. 8, 2012) https://www ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf (Complaint).

otherwise expand the FTC's enforcement authority, the Commission is prepared to share its expertise and assist with formulating appropriate legislation. That said, any such process will involve difficult value judgements that are appropriately left to Congress. Ultimately, no matter the specific laws Congress enacts in the privacy or data security area, the Commission commits to using its extensive expertise and experience to enforce them vigorously, consistent with its ongoing and bipartisan emphasis on privacy and security enforcement.

VI. CONCLUSION

We appreciate the opportunity to comment on ways to advance consumer privacy while fostering prosperity and innovation. The FTC continues to devote substantial resources to this important topic and looks forward to working with NTIA to encourage competition and innovation while protecting consumers.

Justices To Hear TCPA Junk Fax Suit Over 'Free' E-Books

 By **Ben Kochman**

Law360 (November 13, 2018, 10:40 AM EST) -- The U.S. Supreme Court agreed Tuesday to hear a case over whether a district court was right to hold that an unsolicited fax sent by a major health information provider over offers for a free e-book must have a commercial goal to be considered an advertisement under the Telephone Consumer Protection Act.

The high court said it is limiting the certiorari grant to the question of whether the Hobbs Act, in Carlton & Harris Chiropractic v. PDR Network LLC, required the lower court to accept the Federal Communication Commission's legal interpretation of the TCPA. The Fourth Circuit held in February that faxes that offer goods and services, even free goods and services, are "advertisements" under the TCPA, and reversed the district court's dismissal of the suit.

The case is PDR Network LLC et al. v. Carlton & Harris Chiropractic, case number 17-1705, in the U.S. Supreme Court.

--Editing by Alyssa Miller.